

ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ШЛЯХИ ЇХ РЕАЛІЗАЦІЇ

К. В. Лисак

Чернігівський національний технологічний університет, Україна

Науковий керівник О. І. Волот

В сучасних умовах стрімкого розвитку економіки, кожне підприємство для провадження своєї діяльності використовує певну інформацію. Тому протягом останніх років відбувається стрімкий розвиток інформаційних технологій, які значно спростовують та прискорюють ведення бізнесу. Проте спільно з перевагами розвитку інформаційних технологій, виникають ризики виникнення загроз інформаційним

системам, що робить підприємства вразливими. Тому шляхам реалізації загроз інформаційної безпеки повинна приділятися значна роль.

На сьогоднішній день не існує єдиного визначення поняття «інформаційна безпека», тому вважаємо за доцільне привести й узагальнити окремі трактування сутності та змісту цієї дефініції як економічної категорії (табл. 1)

Таблиця 1

Існуючі підходи до визначення сутності та змісту «інформаційна безпека»

Автор	Визначення
В. Цимбалюк [12]	Суспільні відносини щодо створення та підтримання на належному (бажаному, можливому) рівні життєдіяльності відповідної інформаційної системи, у тому числі підприємництва
О. А. Сороківська [9]	Суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності
М. Ю. Танцюра [10]	Як відношення рівня інформаційного захисту до рівня інформаційних загроз; сукупність засобів та дій уповноважених осіб спрямованих на захист інформаційних ресурсів та інформаційної інфраструктури даного підприємства в процесі обміну, обробки та зберігання інформації на всіх рівнях інформаційної системи підприємства
О. І. Крюков [3]	Суспільні правовідносини щодо процесу організації створення, підтримки, охорони та захисту необхідних для особи (людини чи юридичної особи, установи, підприємства, організації), суспільства і держави безпечних умов їх життєдіяльності; суспільні правовідносини пов'язані з організацією технологій створення, розповсюдження, зберігання та використання інформації (відомостей, даних, знань) для забезпечення функціонування і розвитку інформаційних ресурсів людини, суспільства, держави
В. Фурашев [11]	Вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності
С. Гуцу [2]	Стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз
О. Литвиненко [5]	Єдність трьох складових: забезпечення захисту інформації; захисту та контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності

Примітка. Сформовано авторами на основі джерел.

Отже, інформаційна безпека є складним, системним, багаторівневим явищем, на стан якого впливають зовнішні і внутрішні чинники, зокрема політична обстановка у світі; внутрішньополітична обстановка в державі; стан і рівень інформаційно-комунікаційного розвитку країни тощо.

Оскільки інформаційні системи прямо інтегровані в інформаційні структури сучасного підприємства, засоби захисту повинні враховувати відповідні форми представлення інформації. Це означає, що системи захисту повинні забезпечувати безпеку на рівні інформаційних ресурсів, а не окремих документів, файлів чи повідомлень. Тому інформаційну безпеку підприємства слід розглядати у контексті формування безпечних умов існування інформаційних технологій, які включають питання захисту інформації, побудови ефективної інформаційної інфраструктури, інформаційного ринку та створення безпечних умов існування і розвитку інформаційних процесів. Адже, інформаційний захист є значущою складовою інформаційної системи фінансів та бухгалтерського обліку та становить одну з головних функцій сучасної системи управління суб'єктів господарювання [6].

Для забезпечення інформаційної безпеки підприємству необхідно комплексно підходити до захисту та враховувати всі можливі та наявні комп'ютерні загрози. Інформаційна загроза – сукупність умов, випадкове поєднання обставин і подій або наміри об'єкта впливу щодо реалізації ймовірної небезпеки, яка несе деструктивний інформаційний вплив на особистість, суспільство, державу [1].

В науковій літературі зустрічаються різні підходи, щодо класифікації загроз інформаційної безпеки. Проте можна виділити шість основних загроз інформаційній безпеці: розкриття конфіденційної інформації; знищення та спотворення інформації; злом (неправомірне) втручання в роботу; виведення комп'ютерних систем із ладу, зниження їх працездатності; перевищення повноважень непривілейованих користувачів; відмова від авторства та трансакцій [13].

Окремо варто виділити загрози, пов'язані з навмисними помилками, що виникають за межами бізнесу. До таких загроз відносять [7]: несанкціонований доступ до інформації, що зберігається в системі; заперечення дій, пов'язаних із маніпулюванням інформацією; введення в програмні продукти і проекти «логічних бомб», які спрацюють за виконання певних умов або після закінчення певного періоду часу і частково або повністю виводять з ладу комп'ютерну систему; розроблення і поширення комп'ютерних вірусів та інші.

В табл. 2 наведено методи захисту інформації, які умовно можна поділити на декілька груп.

Таблиця 2

Методи захисту інформації

Метод	Зміст
Правовий	Сукупність законів, які регулюють відносини та визначають відповідальність осіб з приводу використання інформації в діяльності підприємства
Апаратний	різні електронні, електронно-механічні та інші пристрої, які вмонтовуються в серійні блоки електронних систем обробки і передачі даних для внутрішнього захисту засобів обчислювальної техніки: терміналів, пристроїв введення та виведення даних, процесорів, ліній зв'язку
Організаційний	Полягає в забезпеченні збереженні конфіденційної інформації підприємства, шляхом формування корпоративної системи захисту
Фізичний	Засоби, які необхідні для зовнішнього захисту обчислювальної техніки, території та об'єкту

Метод	Зміст
Програмний	вмонтовані до складу програмного забезпечення системи, необхідні для виконання логічних та інтелектуальних функцій захисту. Можуть входити в стандартний набір поставки програмного продукту або бути розробленим підприємством індивідуально

Примітка. Систематизовано авторами на основі джерел [4], [8].

Отже, в сучасних умовах стрімкого розвитку значно зростає важливість використання інформаційних технологій, тому питання забезпечення інформаційної безпеки є надзвичайно важливим. Для цього необхідно застосовувати комплексну систему заходів захисту, що полягає в постійному нагляді за джерелами загроз та необхідністю здійснювати захист інформаційних технологій різними способами. Забезпечення інформаційної безпеки повинно розглядатися підприємством як важливий елемент управління процесу управління підприємством.

Література

1. Автоматизація виявлення та протидії інформаційним загрозам у мережі Інтернет / Р. В. Гришук [та інш.] // Наукоємні технології. – 2018. – № 2. – С. 158–165.
2. Гуцу, С. Ф. Правові основи інформаційної діяльності: навчальний посібник / С. Ф. Гуцу. – Х. : Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2009. – 48 с.
3. Крюков О. І. Інформаційна безпека держави в умовах глобалізації / О. І. Крюков // Державне будівництво. – 2007. – № 2. – Режим доступу: http://nbuv.gov.ua/UJRN/DeBu_2007_2_1.
4. Легомінова, С. В. Теоретичні засади інформаційної безпеки підприємства / С. В. Легомінова // Економіка. Менеджмент. Бізнес. – 2015. – № 3. – С. 87–92.
5. Литвиненко, О. В. Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії) : автореф. дис. на здобуття наук. ступеня канд. політ. наук: спец. 23.00.04. / О. В. Литвиненко. – К., 1997. – 18 с.
6. Проблеми інформаційної безпеки суб'єктів господарювання в Україні та можливі шляхи їх вирішення в сучасних умовах / Т. В. Микитенко [та інш.] // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського. – 2016. – № 2. – С. 24–31.
7. Нехай, В. А. Інформаційна безпека як складова економічної безпеки підприємств / В. А. Нехай, В. В. Нехай // Науковий вісник Міжнародного гуманітарного університету. Серія: Економіка і менеджмент. – 2017. – Вип. 24 (2). – С. 137–140.
8. Северина, С. В. Інформаційна безпека та методи захисту інформації / С. В. Северина // Вісник Запорізького національного університету. Економічні науки. – 2016. – № 1. – С. 155–161.
9. Сороківська, О. А. Інформаційна безпека підприємства: нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко // Вісн. Хмельницьк. нац. ун-ту. Сер.: Екон. науки. – 2010. – № 2. – Т. 2. – С. 32–35.
10. Танцюра, М. Ю. Забезпечення ефективності системи інформаційного забезпечення підприємства (на прикладі туристичних підприємств АР Крим) : автореф. дис. на здобуття наук ступеня канд. екон. наук: 08.00.04 / М. Ю. Танцюра. – Сімферополь, 2012. – 21 с.
11. Фурашев, В. М. Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки / В. М. Фурашев // Інформація і право : науковий журнал. – 2012. – № 1 (4). – С. 46–56.
12. Цимбалюк, В. Інформаційна безпека підприємницької діяльності, визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації) / В. Цимбалюк // Підприємництво, господарство і право. – 2004. – № 3. – С. 88–91.
13. Черевко, О. В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту / О. В. Черевко // Ефективна економіка. – 2014. – № 5. – Режим доступу: <http://www.economy.nayka.com.ua/?op=1&z=3304>.